Comprehensive Security Briefing (SEC150)

for

Employees, Contractors, and Consultants

Albuquerque, New Mexico
January 2006-January 2007

Sandia National Laboratories
SAND2006-1442P

Table of Contents

Who is required to take a Comprehensive Security Briefing?

If…

- You are receiving an **"L"** or **"Q"** badge from **Sandia National Laboratories/ New Mexico** (SNL/NM) for the **first time** since being granted a clearance,
- Your clearance is **reinstated** or being **transferred** from another facility.

Using this Booklet

Sandia is continually revising Corporate Process Requirement (CPR) documents to capture the latest requirement changes based on Department of Energy (DOE) orders, federal and state laws, and Sandia best-management practices. When there is a discrepancy between the CPRs and training, follow the information within the CPRs.

This booklet discusses the important role you play in protecting national security. You have been the subject of a personnel security investigation that was conducted to determine your suitability for access to classified matter. You have been granted access authorization (commonly referred to as a security clearance) because Sandia may require you to access classified matter or you require unescorted access to security areas.

You should become familiar with the contents of this booklet. Your manager will give you specific information about security practices for your individual job and area.

The following symbols will aid in guiding you through this booklet:

Key Points –

The most important points that you need to know about each topic.

Notes –

Specific information of an essential nature.

Your Responsibilities –

Things that you are required to do.

For Your Information –

Contact information or resources for more details on each topic.

Introduction

Purpose of this Security Briefing Booklet

This booklet provides information required by DOE Order (O) 470.4, *Safeguards and Security Program,* and DOE Manual (M) 470.4-1, *Safeguards & Security Program and Planning*.

As a Member of the Workforce (MOW) (employee, contractor, or consultant), you have been the subject of a personnel security investigation. The purpose of this investigation was to determine your trustworthiness for access to classified information. By being granted a security clearance, you have met the first of three requirements to have access to classified information.

Classified Information Nondisclosure Agreement

The second requirement you must fulfill in order to have access to classified information is to sign the Standard Form 312 (SF 312), "Classified Information Nondisclosure Agreement," found at the back of this booklet. This form is a contractual agreement between the U.S. Government and you, in which you agree never to disclose classified information to an unauthorized person. The primary purpose of SF 312 is to inform you of (1) the trust that is placed in you by providing you access to classified information; (2) your responsibilities to protect that information from unauthorized disclosure; and (3) the consequences that may result from your failure to meet those responsibilities.

Upon receiving your comprehensive briefing, you should:

- Read the SF 312.
- Sign SF 312 in the presence of an authorized witness. At Sandia/NM, Badge Office personnel are the only individuals authorized to witness your signature.
- Hand the signed form to the authorized witness.

Need to Know

The third and final requirement is having a Need to Know; that is, you must have a Need to Know to acquire the information in order to perform your official duties. As a person with a security clearance, you are personally responsible for all classified matter and Unclassified Controlled Information (UCI) (sensitive matter) entrusted to you. As a holder of classified information, you are responsible for deterring a requester's identity, clearance, and Need to Know. MOW without a clearance are allowed to access UCI as long as they have a Need to Know.

Security Objectives

As a person with a security clearance (clearance), you are personally responsible for all classified matter and UCI entrusted to you. MOW without a clearance are allowed to access UCI as long as they have a Need to Know. Allowing access to UCI is not dependent upon clearance – the clearance is only for accessing classified material.

The DOE and SNL/NM have four major security objectives that you should make your own:

1. **Protection of Special Nuclear Material (SNM)**

   As a Class "A" facility, SNL/NM could have SNM, such as uranium and plutonium in various forms, in its inventory at any time. Control and protection of SNM is essential because of its potentially damaging use should it fall into unauthorized hands.

2. **Protection of Classified Matter**

- To ensure that there is no compromise, unauthorized disclosure, or loss of classified information or material, you shall:
  - Be able to identify unattended classified matter.
  - Know the appropriate reporting requirements. (Reporting requirements are covered on pages 22-24.)
- Before allowing access to such matter, you shall establish the requestor's:
  - Identity (examine the person's badge).
  - Proper clearance access.
  - Official Need to Know.

3. **Protection of Unclassified Controlled Information (UCI)**

   UCI is sensitive matter that can aid unauthorized sources in gaining valuable information to do harm to our national security. Be alert! Protect all sensitive information from unauthorized sources.

4. **Protection of Government Property**

   All property at SNL/NM is owned by DOE and, in essence, the American people. The care of this property is the responsibility of all who work with it. Equipment and resources entrusted to you in your work shall be given due care and accountability.

Responsibilities Regarding Security Education and Awareness

Manager's Responsibilities

Sandia managers are responsible for:

- Encouraging good security habits in their MOW.
- Promoting the proper protection of classified and UCI, government property, and Sandia assets.
- Integrating security awareness, controls, and requirements into all phases and activities of their projects.
- Ensuring that MOW have appropriate training prior to working with classified matter.

MOW Responsibilities

You should:

- Be aware of any special rules and/or requirements as they apply to your job, building, or area.
- Receive training commensurate with your responsibilities beyond this Security Briefing. For example, you will require training if your job responsibilities include the generation, handling, use, storage, reproduction, transmission (including hand carrying), and/or destruction of classified or UCI, or working with Special Nuclear Material (SNM).

For Your Information

If there is any situation you are unsure of, contact one of the following for clarification:

- Your manager
- Division Security Safeguards & Security (S&S) Coordinator
- Security Police Officer
- Corporate Investigators (845-9900)
- Security Education (844-2697 or 284-2416)
- Security Hotline (845-YESS/845-9377)
- Non-emergency hotline (844-6515)

MOW Required Security Briefings

SNL's Education and Awareness Program provides four briefings, as required by the DOE M 470.4-1, *Safeguards and Security Program Planning and Management*. Listed below are the security briefings required by DOE.

Initial Security Briefing *(SEC050)*

The Initial Security Briefing (SEC050) is given to personnel who receive a DOE security badge prior to being given unescorted access and beginning their duties. The Initial Security Briefing:

- Provides basic information about SNL and its S&S program and policies.
- Is for all MOW and given on their initial day of hire.
- Is given to all MOW prior to being issued an uncleared employee badge (grey-striped).

Comprehensive Security Briefing *(SEC150)*

The briefing you are attending today is your Comprehensive Security Briefing (SEC150). You must take this course prior to receiving your cleared badge. This briefing provides:

- More in-depth information on SNL's security operations and requirements.
- Information on your personal security-related responsibilities.

Your Responsibility

Failure to attend this briefing will result in an L or Q badge **not being issued** until the briefing has been completed.

Exemption to the live briefing requirement is permitted on a case-by-case basis for certain off-site MOW.

Annual Security Refresher Briefing *(SEC100)*

MOW with a DOE clearance must complete the Annual Security Refresher Briefing (SEC100) within 12 months of the Comprehensive Security Briefing (SEC150), and every 12 months thereafter, as long as they maintain their security clearance. This briefing:

- May be completed on-line or by hardcopy.
- For contractors – is a shared responsibility between your Line manager and your employer.
- For consultants – is the responsibility of your Line manager.

Termination Briefing *(SEC225)*

The Termination Briefing (SEC225) emphasizes your continuing responsibility not to disclose classified information or matter to which you have had access to during your employment at SNL. The Termination Briefing will also impart potential penalties for noncompliance and your obligation to return all unclassified controlled and classified documents and materials in your possession. This briefing is held when one of the following three events occur:

- Last day of your employment.
- Last day you possess an access authorization.
- Day it becomes known that you no longer require access to classified information or SNM.

Security Areas

Security Areas are a physically defined space identified by posted signs, and some form of access control, which contain special nuclear material (SNM), classified matter, or property. All spaces owned and/or leased by SNL/NM falls within the following security areas: property protection, limited, and protected.

Types of Security Areas

- **Property Protection Areas (PPAs)** – established for the protection of DOE property.
- **Limited Areas** – security areas having boundaries identified by barriers for the protection of classified information.
- **Exclusion Areas –** security areas requiring additional Need to Know authorization and usually requiring that permission be obtained before entering.
    - Provide access to classified information.
    - Allow access to both Q and L clearance holders. However, some areas of an Exclusion Area may be off-limits to an L-cleared person.
    - Check for posted signs in the areas being accessed.
    - Challenge others for proper access level in areas where visitors may be present.
- **Material Access Areas (MAAs)** – established for the protection of SNM.

Search Policy

Upon entering or leaving Sandia-controlled premises, all personnel are subject to search of their persons, hand-carried items, and vehicles to ensure that:

- No contraband is being introduced.
- No government property or classified information/material is being removed without proper authorization.

A Security Police Officer may ask you to submit all containers for examination. Containers include packages, boxes, briefcases, handbags, etc.

Prohibited Items

Items prohibited on Sandia-controlled premises without prior authorization include:

- Firearms
- Explosives, pyrotechnics, propellants
- Illegal drugs and paraphernalia, intoxicants
- Other items prohibited by law
- Personally owned items prohibited within Limited and more restricted areas without prior authorization include:
    - Radio frequency-transmitting equipment
    - Recording equipment (audio, video, data, etc.)
    - Computers, peripherals, associated media
    - Cell phones
    - Portable electronics (including hand-held computing devices)
- A sign regarding prohibited and controlled items is posted at all access gates

For additional requirements and information, see CPR400.2.10, *Using Information Technology (IT) Resources,* Section 4.8, "Prohibited and Controlled Electronic Devices and Media;" CPR400.3.11, *Access Controls*; and CPR400.3.16, *Cellular Phones*.

Personal Vehicle Access

- MOW personal vehicles are not permitted in Limited Areas.
- **Exceptions (up to 180 days)**, such as for health reasons, shall first be approved by Medical, CPR300.5.7, *Medical Restrictions.*
- If you have a **state-issued handicap placard** and require **parking inside a Limited Area**, call 844-4584.

Private and contractor company vehicles are always **subject to search** upon entering and exiting Limited Areas.

After Hours

Note

- After normal working hours most buildings at SNL are locked and alarmed.

Many buildings are controlled by an access-control system; presence of the system is indicated by badge-swipe equipment and/or a keypad for entering a personal identification number (PIN). Some buildings are controlled 24 hours a day and some are controlled only after working hours.

Your Responsibility

- If you need access to a corporate access-controlled building, contact the building manager and ask to be added to the access list.

Ask the building manager for proper exiting procedures for times when you must work after hours. Some access-controlled buildings are configured in such a way that you do not have to call Security first before leaving the building after hours. Some buildings, however, do require that you notify Security first; the numbers to call are 844-4657 (Tech Areas I and II) or 845-3114 (Tech Areas III and V).

For Your Information

- If you find yourself within a building or an area where there appears to be no way out, you should look for a turnstile or locate a phone and call for assistance.
- The Key Service number is 844-4657 (Tech Areas I and II) or 845-3114. (Tech Areas III and V).
- The emergency number is 911.
- Most phones have these numbers posted near them.
- **Do not** exit the building or area by any means other than the conventional way.

Counterintelligence

SNL's Counterintelligence Mission

Sandia's Office of Counterintelligence mission is to protect DOE and SNL interests from foreign and domestic intelligence and economic espionage threats using a centrally directed and managed counterintelligence program consisting of awareness/education, briefings, debriefings (data collection), intelligence community liaison/investigative assistance, and data analysis.

Counterintelligence Reporting Requirements

- Notify the Office of Counterintelligence if you:
  - Have a substantive interaction with a sensitive country foreign national.
  - Are approached or contacted by anyone requesting classified/sensitive information.
  - Suspect you have been approached by a Foreign Intelligence Service (FIS), become an FIS target, or if you have knowledge or information of FIS targeting or recruitment attempts.
  - Receive unsolicited e-mail directed to you from a sensitive country foreign national.
  - Are approached by anyone (*including SNL employees*) who is seeking information for which they do not have a Need to Know.
- Substantive interactions are:
  - Personal contacts that involve sharing of private information and/or the formation of emotional bonds.
  - Professional conversations that generate discomfort because of the sensitivity of the subject being discussed.
  - Business or financial interactions with sensitive country foreign nationals.

For Your Information

For further information about Counterintelligence, consult Office of Counterintelligence (00301).

Operations Security (OPSEC)

National Security Decision Directive 298

In 1988, President Ronald Reagan issued National Security Decision Directive 298 (NSDD 298), which established a National Operations Security (OPSEC) Program. The directive details how each executive department and agency assigned or supporting national security missions with classified or sensitive activities shall establish a formal OPSEC program.

The directive describes OPSEC as a systematic and proven process by which the U.S. Government and its supporting contractors can **deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities.**

DOE complies with the directive through DOE M 470.4-4, *Information Security*, Section B, "Operations Security."

SNL/NM's OPSEC Program

The **purpose** of SNL/NM's OPSEC Program **is to develop OPSEC techniques and measures to enhance the safeguarding of classified, UCI, and proprietary information against unauthorized disclosure or inadvertent release to unauthorized personnel.** Thus, OPSEC is a set of procedures and methodologies that provide a way for program, project, or facility managers to implement cost-effective measures to protect programs and staff from exploitation by adversaries.

- The **key to effective OPSEC** is to determine both what critical information most needs to be protected and how a potential adversary would most likely attempt to exploit weaknesses to obtain that information.
- The OPSEC Program applies to all classified and sensitive activities conducted at SNL/NM.
- OPSEC's five-step process is to:
  1. Identify critical information
  2. Analyze threats
  3. Analyze vulnerabilities
  4. Assess risk
  5. Apply appropriate countermeasures

Key Points

- The five primary categories in which adversaries collect intelligence are:
  - Human Intelligence (HUMINT) – Derived from or collected by human resources.
  - Open Source Intelligence (OSINT) – Information gathered from public sources, such as the internet, environmental impact statements, TV, and radio.
  - Imagery Intelligence (IMINT) – Imaging from satellites to hand-held cameras.
  - Signals Intelligence (SIGINT) – Signals from communications: voice, video, Morse code, and fax.
  - Measurements and Signature Intelligence (MASINT) – Quantitative and qualitative analysis of data from technical sensors.
- Adversaries thrive on collecting many pieces of information they can pull together—like combining puzzle pieces—to discover information about critical programs. A strong OPSEC foundation is built on:
  - Steps taken daily to protect your information, which will lead to a life-long habit of practicing good OPSEC.
  - Team effort—an OPSEC program is only as strong as its weakest player.
  - The individual who is informed and aware is the most important part of an OPSEC program.

Practice OPSEC when:

- Using non-secure telephones and fax machines.
- Working with computers and e-mail communications.
- Holding casual conversations at work or off-site after hours.
- Disposing of trash or recycled paper.
- Conducting routine business activities.

OPSEC Reviews:

- Will be performed in each organization that handles sensitive information at a frequency designated by Section B of DOE O 470.4-4, *Operations Security*.
- Are conducted to determine the level of OPSEC support required by a program or facility.
- Are *fact finding*, not fault finding, and will provide organizations with the details needed to make informed decisions regarding future OPSEC support.

For Your Information

For further information on OPSEC, contact the OPSEC Coordinator (844-5244) or the OPSEC Administrator (844-6640).

Foreign Interactions

Foreign National Access

- Uncleared Foreign National site-specific badges have a red background.
- MOW who provide foreign nationals access to unclassified information, technologies, programs, and SNL sites are required to submit a Foreign National Request (FNR) Security Plan for approval, prior to interaction taking place, as specified in the FNR Security Plan Decision Flow Diagram, and in accordance with applicable time requirements noted in CPR400.3.5, *Foreign Interactions.* For further assistance, call the Foreign Interactions Office (4233-3) help line (844-8263).

Key Points

- **Attention:** Foreign Nationals may be vouched into a Limited Area only by an authorized host, co-host, or escort listed on the approved FNR Security Plan, and only when the approved area is listed on the FNR Security Plan.
- Individuals with red badges are required to have an approved FNR Security plan that documents **all** of the following:
  - Individuals who are approved to host, co-host, and/or escort the foreign national.
  - Approved buildings and rooms.
  - Approved access dates.
  - Approved scope of work.
- Forms and requirements on interacting with foreign nationals can be found on Sandia's Internal Web, on the Foreign Interactions Office Homepage at http://www-irn.sandia.gov/security/fio/.

For Your Information

For further information, details, or requirements about foreign national policies and procedures, call the Foreign Interactions Office help line (844-8263).

Foreign Travel

Reporting Foreign Travel

DOE requires that Sandia MOW obtain approval for all official foreign travel prior to departure. This includes sensitive, non-sensitive, DOE-funded, WFO (reimbursable), and travel funded by indirect monies. DOE also requires that unofficial (personal) travel to sensitive countries be reported by all individuals who hold a DOE clearance. Specifically, the time limits for submitting business-related foreign travel trip requests to the Foreign Travel Office are as follows:

Key Points

- Non-sensitive official foreign travel – 37 days prior to departure date.
- Sensitive official foreign travel – 52 days prior to departure date.
- All official foreign travel must be approved through the Foreign Travel Office and DOE, prior to departure.
- For details and requirements consult the Foreign Travel help line (845-1300).
- Be aware that there are many restrictions regarding the equipment you may take on foreign travel and that a long lead time is necessary when planning trips. Contact the Import Control Office (844-7112).
- All MOW (regardless of whether they hold a DOE clearance and anyone [e.g., contractor, consultant] who currently holds a DOE security clearance) shall report all foreign travel to sensitive countries through the corporate Travel Information System (TIS) prior to departure or as soon as practical.
- A list of DOE **sensitive foreign countries** may be found at http://www-irn.sandia.gov/security/dept/fio/fio_countries.htm.
- Caution should be exercised in dealing with citizens of any country to ensure that sensitive information, although unclassified in nature, is not inadvertently disclosed. This would include nuclear and other U.S. technology and economic information.

For Your Information

For further information about foreign travel, call the Foreign Travel help line (845-1300).

Classifying Information

Why We Classify

- All classified information/material is protected according to federal statutes and Presidential Executive Orders. DOE is responsible, under the Atomic Energy Act of 1954, as amended, for classifying information and material relating to atomic energy and its use in weapons, and under Executive Orders for other aspects of national security. The Atomic Energy Act of 1954 and Executive Order 12958 govern classification policy.
- Classifying establishes protective barriers that ensure that classified information and material do not fall into unauthorized hands. Through the process of classification, we protect important information from adversaries yet allow the same information to be used by scientists, statesmen, military planners, and others with applicable access authorization and the Need to Know.
- A derivative classifier (DC) determines the appropriate classification level, category, and any required caveats. The classification process is particularly crucial to DOE because its responsibilities include the development and production of nuclear weapons.

Categories of Classified Matter

Information and material are classified based on categories and levels:

- **Categories** – specify the types of information or material.
- **Levels** – indicate the sensitivity and degree of damage that could incur to national security should that information or material be compromised.

Key Points

There are **three categories** of classified matter:

1. Restricted Data (RD)

All data concerning design, manufacture, or utilization of atomic weapons; the production of SNM; or the use of SNM in the production of energy, but shall **not** include data declassified or removed from the RD category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended. Examples of technologies categorized as RD are nuclear assembly design, firing and detonating systems, initiators, nuclear safing mechanisms, inertial confinement fusion, and isotope separation. RD is, generally, the most restrictive of the three classification categories.

2. Formerly Restricted Data (FRD)

Classified information jointly determined by the DOE or its predecessors and Department of Defense (DoD), to be related primarily to the military utilization of atomic weapons, and removed by the DOE from the RD category pursuant to Section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to RD. Examples of technologies of the FRD category are fuzing designs, weapons yields, weapon location information, command and control systems, and certain other information the military needs to carry out its nuclear weapons responsibilities.

3. National Security Information (NSI)

Information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure, is so designated.

The levels, Top Secret, Secret, and Confidential, are used to designate the sensitivity of information. Examples are information related to S&S, nuclear reactor site security, and weapon carriers (e.g., missile and aircraft units).

Levels of Classified Information and Matter

The classification level indicates how sensitive the information or material is.

Key Points

- There are **three levels** of classified information or matter:

1. Top Secret (TS)

Unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security in a way that the appropriate official can identify or describe.

2. Secret (S)

Unauthorized disclosure could reasonably be expected to cause serious damage to national security in a way that the appropriate official can identify or describe.

3. Confidential (C)

Unauthorized disclosure could reasonably be expected to cause undue risk to the common defense and security in the case of RD/FRD, or damage national security in the case of NSI, in a way that the appropriate official can identify or describe.

Information and materials vary in their importance to national security. The greater the risk of damage to national security if disclosed to unauthorized sources, the **more sensitive** the information is considered to be, and the higher the level of classification it has.

General Guidelines

- Only one classification for an entire classified work can exist, and that classification shall be the highest classification **category** and **level** of any part of the work.
- Multiple classifications **cannot** exist for complete documents or materials, although the individual "parts" of the document or material may have different classifications.
- RD and FRD do not normally require portion marking.
- NSI documents are required to be portion marked.

Determining Proper Classification

- Derivative Classifiers (DCs), many of whom are managers and experts in their field, are the only persons authorized to make classification determinations.
- Unclassified Controlled Nuclear Information (UCNI) Reviewing Officials (ROs) are the only persons authorized to determine that a document is UCNI. Many of the DCs are also UCNI ROs.
- You may seek the assistance of classification analysts, who also are DCs, in the Classification Department (4225), when necessary.

For Your Information

For more information on Classification, consult the Classification Homepage: http://www-irn.sandia.gov/security/dept/classification/, or one of the Classification Analyst in the Classification Department (4225).

Unclassified Controlled Information (UCI)

DOE and other federal agencies require that controls be placed on the availability of certain scientific and technical information even though the information is not classified. This type of sensitive information is described as UCI.

Key Points

There are **three** basic types of UCI. They are:

- **Official Use Only (OUO)**
  - You will receive additional training on OUO at a later date.
- **Unclassified Controlled Nuclear Information (UCNI)**,
  - UCNI is certain unclassified Government information whose unauthorized dissemination is prohibited under Section 148 of the Atomic Energy Act. Due to information sensitivity, failure to protect UCNI may lead to a Security Incident.
- **Naval Nuclear Propulsion Information (NNPI)**
  - Corporate owned information is also a type of UCI.
  - As with classified information, access to UCI information is limited to those with a Need to Know, who need it for the performance of their official or contractual duties and who have had the proper training.

For Your Information

The following link takes you directly to the UCI information on the Classification Department's (4225) Homepage: http://www-irn.sandia.gov/security/dept/classification/uciunclass.htm

Media Relations

Media Relations

Public media reports of classified work at SNL/NM should **not** be affirmed, denied, or commented upon.

Applicable requirements on media relations can be found in the Sandia CPR200.1.1, *Media Relations*.

Classified Matter Protection and Control (CMPC)

As a newly cleared individual, you should be familiar with the "cradle-to-grave" concept used in the Classified Matter and Protection Control (CMPC) program. If your work responsibilities involve handling classified matter, you must receive additional training beyond this security briefing. Not every MOW at SNL/NM works with, or comes in contact with classified matter.

Controlling Classified Matter

- Control classified matter against unauthorized access at all times.
- Immediately report incidents involving classified matter, including lost or unaccounted for classified matter, to your manager. If your manager is not available, report the incident to another member of management or OOPS (311). Then ensure that the incident is immediately reported to the Security Incident Management Program (SIMP) (24-hour pager: 540-2382).

For Your Information

Be particularly careful not to divulge classified information when reporting any security incident.

- Manage classified matter in established control stations assigned to an appropriate Classified Administrative Specialist (CAS).

Accessing Classified Matter

- Access to classified matter is the responsibility of the owner of the information.
- Ensure MOW have the proper clearance level and Need to Know before permitting them to have access to classified matter.

Creating Classified Matter

- Classified matter shall be marked appropriately. Originators shall have proper classification review performed and apply proper marking requirements on drafts and final documents.
- CAS assists in reviewing markings and with marking classified matter.
- Appropriate cover sheets shall be used.

Using Classified Matter

- Whenever classified information is in use, it shall be:
  - Within line of sight.
  - Under personal attendance.
  - Have a cover sheet.
- Control may be relinquished only to those who have the appropriate clearance and Need to Know.
- Reproduce classified in coordination with the CAS.
- Only the minimum number of copies for operational necessity may be prepared.

- Copier shall be approved to copy classified.
- Marking of classified matter is the responsibility of the originator.

Storing Classified Matter

- Protect classified matter by securing it in an approved repository when not in use.
- Approved repositories are GSA-approved safes, approved vaults, and vault-type rooms (VTRs).
- Ensure CAS knows where classified is stored.

FYI For Your Information

Technical Security (4214) installs, designs, and maintains the building alarms, vault and VTR alarms, and badge readers at all entry-controlled access points, as well as on vaults, VTRs, and other restricted-access areas. For additional information, consult Technical Security (4214).

Moving Classified Matter

- Mail, ship, or hand-carry classified matter only to authorized recipients and those with a Need to Know.
- Use SNL mail and shipping services only to mail and ship classified matter.
  - Internal recipients shall have an approved control station.
  - External recipients shall have a DOE-approved Mail/Shipping Channel.
- If classified information has access control markings, the originator shall ensure that the intended recipient has the appropriate access authorization for that information (e.g., Weapon Data, NOFORN).
- Hand-carry classified matter as a last resort and only if you have:
  - An active, DOE-approved Mail Channel at the destination.
  - Taken the Annual Hand-Carry Briefing (SF 2902-AHB).
  - Written authorization from your manager.
- Double wrap documents or use SNL-authorized double hand-carry bags when transporting classified documents outside of a Limited Area.
- Receipts for classified matter shall be created and signed, as required in CPR400.3.12, *Management of Classified Matter*.
- Always work with your CAS.

FYI For Your Information

Direct questions regarding Mail or Shipping Channels to the Mail Channel Coordinator (4234-3) at 844-8952.

Destroying Classified Information

- Destroy classified matter in accordance with the Sandia Records Retention and Disposition Schedule.
- Coordinate destruction with the appropriate CAS.
- Use destruction methods that are approved to ensure classified matter is physically altered, demolished, or reduced to a useless form in such a way that no classified information can be obtained from it.
- Always work with your CAS.

Accountable Classified Removable Electronic Media

Accountable Classified Removable Electronic Media (ACREM) are those materials and components manufactured for the purpose of providing non-volatile storage of classified digital data capable of being read by a computer. "Removable" refers to such media that:

- Are designed to be introduced to and removed from the computer without adverse effect on computer functions.
- Can be separated from the computer for any reason.
- Are portable electronic devices, including laptop computers with fixed internal hard drives.

CREM becomes Accountable Classified Removable Media **(**ACREM**)** when it stores one of the following types of information

- Top Secret (TS)
- Secret Restricted Data (SRD)
- All Sigma 14 and Sigma 15

ACREM may also be removable electronic media that are accountable because of national, international, or programmatic requirements that include:

- Deployable classified computer equipment and media supporting Nuclear Emergency Search Team (NEST) and Accident Response Group (ARG) Operations
- Cryptography and designated Communications Security (COMSEC)
- NATO ATOMAL
- Designed United Kingdom (UK) information
- Foreign Government Information designated in international agreements
- Special access programs
- Any electronic media with write capability, when introduced to an SRD or higher system.

Your Classified Administrative Specialist (CAS) is required to strictly control ACREM and to enter ACREM into a formal, approved accountability system.

ACREM Requirements

MOW shall:

- Accept responsibility for all ACREM checked out to them per, CPR400.3.12.3, *Management of Accountable Classified Documents at SNL/NM and Remote Sites*, Attachment H, "SNL ACREM Check In/check Out Procedure."
- Know the requirements for managing ACREM.
- Ensure that ACREM within their control, regardless of form, are afforded a level of protection against loss or compromise commensurate with its level of classification.

- **Not** allow others to borrow or use ACREM that they have checked out from the CAS.
- Ensure that classification levels and categories of ACREM are appropriate for the computer system accreditation level used to process the data.

Additional information and requirements on ACREM can be found in CPR400.3.12.3, *Management of Accountable Classified Documents at SNL/NM and Remote Sites*, Attachment D, "Accountable Classified Removable Electronic Media."

For Your Information

For questions regarding classified information or material, consult the Classified Matter Protection & Control Program in Information Security (4234).

Material Control and Accountability (MC&A)

Material Control & Accountability (MC&A) Program

As part of Sandia's authorization to possess and use accountable nuclear material, Sandia must provide an effective MC&A Program. Sandia's Program is responsible for managing certain aspects of accountable nuclear material. This responsibility includes generating and maintaining accurate information regarding nuclear material quantity, location, and other characteristics, as well as reporting information to the DOE's national nuclear material database.

Types of Accountable Nuclear Material

Accountable nuclear material is divided into three types:

- Special Nuclear Material (SNM)
- Source Nuclear Material
- Other Nuclear Material

Note

For the purpose of this Security Briefing, only SNM is defined.

SNM is fissionable nuclear material (such as enriched uranium or plutonium), which releases energy when its atoms are split. Because of this capability, SNM is used for nuclear weapons. SNM must be guarded to prevent possible theft or sabotage.

All accountable quantities of nuclear material are required to be controlled, inventoried, measured, and tracked through an accountability (database) system. The nuclear material must be located in a Material Balance Area (MBA). The amount of SNM is characterized by "category." Category I is the highest quantity and Category IV is the lowest quantity group. A Category I or II quantity of nuclear material requires a higher level of physical security protection that includes a protection area named a material access area (MAA).

Management of accountable nuclear material helps ensure the material is properly characterized, controlled, protected, used, and accounted for, thereby deterring and detecting theft, diversion, or unauthorized use of nuclear material.

Training For Accountable Nuclear Material Handlers

Individuals who access accountable nuclear material, that is handlers, MBA custodians, nuclear material project representatives, testers, or experimenters, are required to take Accountable Nuclear Material User Training (SEC120).

For Your Information

For additional information on Sandia's MC&A Program, click on MC&A Department's (4216) Homepage: http://www-irn.sandia.gov/security/dept/mca/, or reference CPR400.3.14, *Management of Accountable Nuclear Material.*

Reporting Requirements

General Reporting Requirements

Executive Order 12968, *Access to Classified Information*, makes a very serious demand on **ALL** MOW. It states:

"Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security."

A common concern is, "What issues raise doubt about a person's eligibility to be trusted with national security interests?" They are the same issues that were considered when you were being investigated for your clearance.

Your Responsibility

It is your duty and responsibility to:

- Maintain your access authorization.
- Report any doubts about the trustworthiness of those people you work with and around.

Supervisor's Reporting Requirements

Supervisor's Reporting Requirements:

- In compliance with CPR400.3.7, *Security Concerns Reporting Process*, and DOE M 470.4-5, *Personnel Security*, **ALL** supervisors aware of the following conditions affecting an applicant's or employee's access authorization status, shall provide notification of:
  - An individual's hospitalization for a mental illness or other condition (e.g., substance or alcohol abuse) that may cause a significant defect in the individual's judgment or reliability. Verbal notification must be made within 8 working hours and written confirmation within the next 10 working days.
  - Information of personnel security interest.
  - Such information must be characterized as reliable and relevant and create a question as to an individual's access authorization eligibility as described in 10CFR710.8, *Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material*.

Note

Verbal notification shall be provided within 2 working days and written confirmation within the next 10 working days to Corporate Investigators (845-9900).

For Your Information

For more information regarding DOE reporting requirements, consult the following:

- Corporate Investigators (845-9900).
- Personnel Security/Badge Office (844-8742).
- CPR400.3.7, Security Concerns Reporting Process.

Maintaining Your Access Authorization

Maintaining your security clearance is essential to your job.

- In order to maintain your security clearance, you shall follow all reporting requirements, which apply both within and outside of the United States.

IF YOU	YOU SHALL REPORT THIS	TO
• Are arrested, have criminal charges brought against you (including charges that are dismissed), or detained by Federal, state, or other law enforcement authorities for violations of the law, within or outside of the U.S. **Note:** Traffic violations for which only a fine of $250 or less was imposed do not have to be reported unless the traffic violation is alcohol or drug related.	• **Orally,** within 2 working days of occurrence. • **In writing,** within the next 3 working days.	Corporate Investigators (845-9900)
• File for bankruptcy, regardless of whether it is for personal or business-related reasons.	• **Orally**, within 2 working days of occurrence. • **In writing**, within the next 3 working days.	Corporate Investigators (845-9900)
• Have your wages garnisheed for ANY reason. Examples: divorce, debts, child support.	• **Orally**, within 2 working days of occurrence. • **In writing**, within the next 3 working days.	Corporate Investigators (845-9900)
• Are a Current U.S. Citizen who changes citizenship or dual citizenship. • Are a Foreign Citizen who Changes citizenship. • Name change.	• **Orally**, within 2 working days of occurrence. • **In writing**, within the next 3 working days.	Personnel Security 844-5688 Foreign Interactions Office 844-8263
• Marry or cohabitate in a spouse-like relationship.	• **In writing** (DOE Form 5631.34, *Data Report on Spouse*), within 45 calendar days of marriage or cohabitation.	Personnel Security 284-9519
• Are approached or contacted by ANY individual seeking unauthorized access to classified matter or SNM.	• Immediately.	Counterintelligence (284-5923) **or** Corporate Investigators (845-9900) **or** SIMP Pager (540-2382)

IF YOU	YOU SHALL REPORT THIS	TO
• Are hospitalized for a mental illness or a mental condition, or for treatment of alcohol or drug abuse.	• **Orally,** within 2 working days of occurrence. • **In writing,** within the next 3 working days.	Corporate Investigators (845-9900)
• Have business-related foreign travel to sensitive countries. • Have business-related foreign travel to non-sensitive countries. • Have personal foreign travel to sensitive countries. **Note:** You are not required to report personal foreign travel to non-sensitive countries before your trip; however, keep a personal record of such travel for future clearance investigations.	• 52 days before trip. • 37 days before trip. • Prior to travel, or as soon as practical.	Foreign Travel (845-1300)
• Have contact with persons from sensitive countries. • Are employed by, represent, or have other business-related association with a foreign or foreign-owned interest, or foreign national. **Note:** Contact is defined as "a substantive personal or professional relationship."	• Immediately.	Counterintelligence (284-5923) **or** Corporate Investigators (845-9900)
• Are aware of information of personnel security interest. **Note:** Such information must be characterized as reliable and relevant and create a question as to the individual's access authorization eligibility as described in 10CFR710.8, *Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material*.	• Immediately.	Corporate Investigators (845-9900)

Corporate Investigations Areas of Concern

Waste, Fraud, and Abuse

It is necessary for all MOW to be vigilant in protecting the funds and resources that are entrusted to SNL by our government and customers.

- Incidents of waste, fraud, abuse, and criminal matters shall be reported to SNL Corporate Investigators (845-9900) and other appropriate authorities.
- The Sandia Ombuds and Ethics Offices (844-1744) are also available.

Theft of Property

- Any theft of Sandia or U.S. Government property shall be reported immediately to SNL Corporate Investigators (845-9900).

All property that is considered stolen, lost, or missing shall be reported regardless of value and regardless of whether it is considered controlled or uncontrolled property.

Wrongdoing

- In addition to the circumstances listed in the previous tables (pp.23-24), MOW shall report incidents of wrongdoing to:
  - SNL/NM contacts listed in the previous table.
  - SNL Corporate Investigators (845-9900).

You may also report directly to the Office of the Inspector General any information concerning wrongdoing by DOE employees, contractors, subcontractors, consultants, grantees, or other recipients of DOE financial assistance, or their employees.

Drugs in the Workplace

- Illegal drugs are prohibited on both Sandia-controlled premises and Kirtland Air Force Base property.
- Individuals who illegally used or trafficked in a controlled substance may be asked to sign a drug certification form attesting to refraining from using or being involved with illegal drugs while employed in a position requiring a security clearance.
- The use of illegal drugs is a serious offense and could result in termination of your clearance, and eventually your employment, as well as arrest.

Incidents of illegal drugs in the workplace shall be reported to Corporate Investigators (845-9900). This includes, but is not limited to, trafficking in, selling, transferring, possessing, or using illegal drugs.

Security Violations

Sandia management is responsible for taking corrective action and reporting any security violations in writing to the SNL Corporate Investigators.

- Security violations are a criminal breach of federal law and can be acts of deliberate intent to harm national interests.
- Severe criminal penalties, including termination and imprisonment, or both, may be imposed for security violations.

If you have questions or need details concerning Security Violations, consult the SNL Corporate Investigators.

Suspension/Termination

Key Points

Your access authorization may be suspended or terminated for any of, but not limited to, the following derogatory* reasons:

- Gross misconduct, failure to protect, or careless handling of classified matter.
- Disclosure of classified information to a person unauthorized to receive such information.
- Failure to safeguard SNM.
- Theft of government property.
- Association in any act of sabotage, espionage, treason, terrorism, or sedition.
- Gross violation of or disregard for security or safeguards regulations.
- Illness or mental condition that significantly impairs an individual's judgment or reliability.
- Excessive or habitual use of alcohol.
- Trafficking in, selling, transferring, possessing, or using illicit drugs or controlled substances.
- Engaging in any unusual conduct that reveals an individual as dishonest, unreliable, or untrustworthy.

*10CFR710.8, *Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material*, lists information that is considered "derogatory." This information casts doubt upon the reliability of an MOW to obtain or maintain access authorization to DOE security interests.

Access/Escorting

Clearance Access

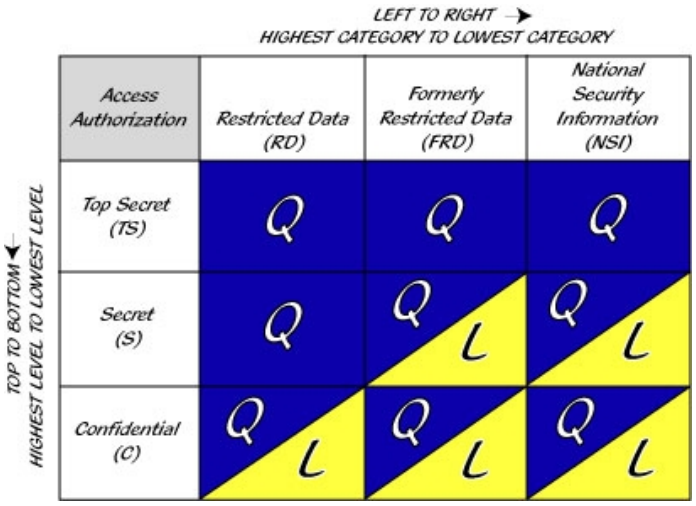
Access, which is provided on a Need to Know basis, is the ability and opportunity to obtain knowledge, use, or possession of classified information required by an individual to perform official or contractual duties. Access is limited to persons with an appropriate clearance level and a Need to Know in order to accomplish work assignments.

Need to Know

Need to Know is determined by persons having responsibility for classified information/material and UCI, thus, allowing access to such information/material as necessary in the performance of official or contractual duties.

Security Badges

- All MOW are issued DOE standard badges.
- Access to classified information/material is granted with the appropriate clearance level and on a Need to Know basis.
- The most common clearances granted by the DOE at SNL are the "L" and "Q." The access authorization permitted by each is:
    - Secret Formerly Restricted Data (SFRD)
    - Secret National Security information (SNSI)
    - Confidential Restricted Data (CRD)
    - Confidential Formerly Restricted Data (CFRD)
    - Confidential National Security Information (CNSI)
    - SNM Categories II and III
    - Unescorted access to Limited and Protected Areas
- A "Q" clearance (blue badge) allows access to all of the above, plus:
    - Top Secret Restricted Data (TSRD)
    - Top Secret Restricted Data (TSFRD)
    - Top Secret National Security Information (TSNSI)
    - SNM Category I (only if individual has Human Reliability Program [HRP] certification, in addition to a Q-clearance and Need to Know)



Your Responsibilities for Your Security Badge

The badge you will receive is an important credential—evidence that a rigorous background investigation found you worthy of being entrusted with our nation's security. Note that the badge comes with additional responsibilities: Bring your badge to work, wear it appropriately at Sandia and other DOE sites, and protect it against theft, loss, and misuse.

- **It is against the law** to counterfeit, alter, or misuse a badge.
- If your badge is lost or stolen, report it immediately to the Badge Office (work hours: 284-3626; after hours: 844-3155). Additionally, it is a requirement that form SA 2730-LSB, SNL Lost/Stolen Badge Report, be completed and turned into the Badge Office, prior to the release of a replacement security badge.
- Your badge is the property of DOE and shall be returned to Personnel Security/Badge Office (4233-1) if it has expired, is no longer needed, or upon termination.
- Do not use the DOE standard badge outside of DOE facilities other than for government purposes. If you need an SNL/NM ID, the Badge Office can supply you with one.
- MOW on extended leave of absence (over 90 days) shall return their badge to the Badge Office and call 284-9773 for additional guidance.
- Upon entering any Sandia Limited Area, present your badge for examination by the Security Police Officer or use the automated gates.
- You shall:
  - **Wear your badge** in plain view, above the waist while in DOE-owned or leased security areas, including Property Protection Areas (PPA).
  - **Renew it** when your contract company or contract number changes.
  - **Renew it** when your name or physical appearance changes.
  - **Renew it** if faded or damaged.
  - **Remove it** when off-site—for example, don't wear your badge to restaurants, or to obtain a gym or an airport parking discount.
  - **Protect it** from theft.

Reinvestigation

Following your initial background investigation, your background is reinvestigated,

- Every 5 years if you hold a "Q" clearance, and
- Every 10 years if you hold an "L" clearance.

Escorting Uncleared Persons or Visitors

- DOE "Q"- r "L"-cleared U.S. citizens can act as escorts.
- Your responsibilities as an escort **anywhere on Sandia-controlled premises** are:
  - **Do not** exceed eight uncleared MOW per escort.
  - Brief uncleared MOW about evacuation procedures and how to report emergencies.
  - Ensure that uncleared MOW are badged through the SNL/NM badge office.
  - Ensure that uncleared MOW follow rules and signs, including those rules and signs that relate to prohibited items.
  - If escort responsibility is transferred, ensure that new escorts are aware of their responsibilities.
  - Ensure that any uncleared person surrenders their badge per instructions on their orange card (SA 2730-CB), and that surrendered badges have been placed in a Sandia badge drop box or taken to the SNL/NM Badge Office.
- Uncleared U.S. citizens with appropriate DOE-approved badges may:
  - Enter Security Areas if they are on official business and are appropriately escorted.
  - Be escorted into Limited Areas for authorized and essential unclassified business activities.
  - Have unescorted access into a PPA.
- Within **Limited or more restricted areas**, only a U.S. citizen (Sandia MOW) with a "Q"- or "L"-clearance and DOE-approved badge may escort.

Escort responsibilities are to:

- Remain with the uncleared MOW at all times.
- Ensure that uncleared MOW **do not** gain access to classified material.
- Inform uncleared MOW of prohibited items.
- Allow access by uncleared MOW through automated gates, using your badge and personal identification number (PIN).
- Notify SNL/NM Security (844-4657 or 844-4658), if visit ends later than 6 p.m.

Note

Uncleared Visitors are required to wear a "site specific" grey-striped badge.

Vouching/Piggybacking

S&S is frequently asked questions regarding MOW using their badges to swipe in other persons. Following are a few of the most frequently asked questions:

- What options do I have when asked to vouch ("piggyback") someone into a Limited Area?
- If the person has an apparently valid "Q" or "L" badge, should you let him or her enter the Limited Area?
- When should you suggest that the person go to a manned gate or to the Badge Office?

There may be various reasons why another individual's badge is not allowing him or her access through an automated access point. The following background sets the stage for the answers to the questions above:

- Badgeholders have become so proficient at swiping badges that 97 percent of all badgeholders are granted access on their first swipe.
- Although there are occasional equipment failures, the general rule is that people who have not gained access after multiple swipes should go to the Badge Office (4233-1) (Building 800).

Key Points

- Vouching (piggybacking) is a term used at Sandia to describe when one person allows another unescorted access.
- When you vouch for another person, it is assumed that you accept the responsibility and consequences of allowing that person into the area.
- At SNL/NM, there have been some experiences of people misusing the vouching privilege. Two examples follow:
  - A person whose badge would not work went to several gates and asked people to swipe him in. Security had deactivated his badge but had not been able to retrieve it. His badge still appeared valid.
  - One person claimed that his badge was left in the Limited Area and asked people to swipe him in so that he could retrieve it.
- Sandia-issued badges have a blue thunderbird in the lower part of the badge.
- DOE badges from other sites **do not** work in SNL/NM's system unless they have been enrolled in the Badge Office (4233-1). After the Badge Office enrolls them, badges from other DOE sites will work in SNL/NM's system.

A "Vouching" Example

As you approach the gate, you notice an individual attempting to gain access through the gate, but failing as he swipes his badge. Frustrated, the individual turns to you and asks if you will "vouch" him in (i.e., swipe your badge to allow the individual to enter unescorted).

Key Points

The questions you must ask yourself are:

- How well do I know this person?
- Is the individual's badge failing to swipe because he,
  - no longer has a clearance but the badge was not confiscated from him?
  - failed to complete their security briefing on time and had his badge deactivated (still has a clearance), or
  - badge is frayed so badly that it will not swipe.

Obviously, if you do not know this person, you should refer him to the badge office. But what if you do know the person, but do not know and can't verify if the individual fits the above criteria? Again, you should refer him to the badge office.

Your Responsibility

- It is appropriate for you to grant access to another person if you feel that you can vouch for her entry into a Limited Area. Before you grant access, ask yourself:
  - How much risk do I want to accept?
  - Is the individual's badge a DOE-approved badge?
- Does the badge look altered in any way?
- How well do I know this person?
- Does the person have an active clearance?

For Your Information

If you feel uncomfortable with your answers to any of these questions, send the person to the Badge Office (Building 800) (844-1206). See CPR400.3.11, *Access Controls*, for additional access requirements and information.

Technical Surveillance Countermeasures (TSCM)

- The purpose of the TSCM Program is to deter unauthorized clandestine technical intelligence collection and to ensure that any overt surveillance is undertaken only under certain circumstances, subject to the requirements of CPR400.3.1, *Technical Surveillance – Audio and Video Recording*.
- TSCM personnel conduct activities under the auspices of the TSCM Program for the purpose of identifying exploitable security weaknesses and enhancing technical and physical security.
- The TSCM Program uses techniques and measures to detect and nullify a wide variety of technologies that are used to clandestinely obtain unauthorized access to classified national security information, restricted data, and/or unclassified controlled information (UCI).

Your Responsibility

- Your responsibilities under the TSCM Program includes reporting suspected technical penetrations or clandestine audio and video equipment immediately, and taking the following steps:
  - Stop all classified or sensitive discussions.
  - Secure the area so that no one can remove or modify the device.
  - Contact the TSCM Team (844-4047) from a location outside the area.
- For additional information about contacting the TSCM Team, see the TSCM section of CPR400.3.1, *Technical Surveillance – Audio and Video Recording*.

Technical Surveillance Equipment (TSE) and Potential TSE (PTSE)

Technical Surveillance Equipment

- An example of what is considered TSE is equipment that is commonly developed for law enforcement actions (e.g., wireless microphones worn on the body, or miniature cameras inserted in clocks). This equipment allows law enforcement personnel to survey criminal activity.
- Some Sandia operations use equipment that was purchased for legitimate business needs, but is capable of being used as TSE in its "as purchased" state. Some examples of this type of equipment would be wireless microphones, wireless cameras, and radio frequency transmitters. Sandia has developed requirements regarding the acquisition, possession, and use of TSE to ensure its proper use. Consult CPR400.3.1, *Technical Surveillance – Audio and Video Recording*, for those requirements.

- TSE may be allowed in OVERT surveillance of business operations, such as part of a Sandia project (e.g., an observation tool to record an ongoing laboratory experiment/project), or for health safety or Environment, Safety & Health (ES&H) concerns. The owners of such devices are required by CPR400.3.1, *Technical Surveillance – Audio and Video Recording*, to ensure that a security plan is developed.
- Areas with active surveillance equipment shall have signs posted to inform MOW of its presence.

Potential Technical Surveillance Equipment (PTSE)

- Current concerns affecting most Sandians are the types of equipment known as PTSE, which includes some commercial equipment that, although not designed to be surveillance equipment, could be used as such if employed illegally.
- In general, PTSE that shall be registered with TSCM, according to CPR400.3.1, *Technical Surveillance – Audio and Video Recording*, consists of portable audio and visual data recording devices. The following list of PTSE is **not** comprehensive and is included here for guidance only.
  - Digital Cameras
  - Video Cameras
  - Scanning Pens and other portable scanning devices
  - MP3 players
  - 35mm Cameras
  - Microphones
  - Palm Pilot-type digital camera or audio recording attachments
  - Dictaphones and digital voice recorders
- Equipment maintained or installed in a Sandia-owned or -controlled PPA is exempt from registration requirements. Local Line management may institute their own control and inventory methods for equipment kept in a PPA. Equipment that is stored, maintained, or installed in a Limited or more restricted area shall be controlled according to CPR 400.3.1.
- For information about exemptions, consult CPR400.3.1, *Technical Surveillance – Audio and Video Recording*. If the equipment is not covered by another CPR and is not exempt, register PTSE by using SF 2925-TSE, Registration of Potential Technical Surveillance Equipment (Potential TSE), or a specially developed plan.

Cellular Telephones

Key Points

- **Non-government-purchased cellular phones** (a.k.a. privately owned) are prohibited inside SNL/NM Limited and Protected Areas but are allowed in some Property Protection Areas.
- Non-government-purchased cellular phones may be permitted in Limited Areas under special circumstances (medical exemptions, etc.). Submit SF 7643-POC, Cellular Phone Approval – Non-Government Phones Within SNL Limited and Protected Areas, for approval.

- Cellular phones owned by other U.S. Government agencies (e.g., DOE, DoD) are not allowed in SNL limited or more restricted areas unless a prior exception has been obtained. Exceptions may be obtained via SF 7643-OTE, U.S. Government Agency Visitor One-Time Exception to SNL Cellular Telephone Requirements.
- **Sandia-purchased cellular phones** must have prior authorization to be stored and used within SNL/NM limited and more restricted areas. Those phones are limited to certain makes and models that have been approved for use in those areas. The phones **shall**:
  - Be registered by submitting SF 7643-PUR, Sandia-Purchased Cellular Phone Security Registration, to TSCM (0301-1).
  - Be authorized for use by TSCM (0301-1). Those phones must have a critical safety or security mission use. Request authorization by filing SF 7643-USE, Cellular Phone Critical Use, with TSCM (0301-1). If approved, a Critical Use Authorization card will be issued.
  - Have a blue Sandia property sticker affixed.
  - Be turned "OFF." Cellular phones may be used only as necessary for safety and security reasons in support of critical operations, or to report an emergency (844-0911).
- A limited number of Sandia-purchased cellular phones are authorized for use in Limited Areas. These shall be registered using SF 7643-USE, Cellular Phone Critical Use.
- Cellular phone users shall comply with Line- and site-specific cellular phone rules and restrictions.
- Call 844-8420 (0301-1) with questions concerning cellular phones.
- For additional information, see CPR400.3.16, *Cellular Phones*.

Note

- While in Limited Areas:
  - Any authorized non-government-purchased cellular phone shall be turned off and locked in a personal or contractor company vehicle authorized to park in the SNL/NM Limited Area.
  - Any Sandia- or government-purchased phone shall be turned off (preferably with the batteries removed) unless properly registered, using SF 7643-USE, Cellular Phone Critical Use.

Personal Data Assistants (PDAs) and Pagers

- **Personally-owned** small electronic items (e.g., Palm Pilots, data organizers, pocket PCs) are **not** permitted in Limited Areas.
- **Sandia- or government-purchased** small electronic items are permitted but shall be identified as such. Some security areas require TSCM inspection of Palm Pilots and other PDAs before they are permitted in the areas.

- Palm Pilots and other PDAs with recording capability (e.g., modem, microphone, camera) should be registered with TSCM using a security plan or SF 2925-TSE, Registration of Potential Technical Surveillance Equipment, if the recording feature has not been disabled or is going to be used in the course of work.
- Palm Pilots and other PDAs with radio frequency (RF)-transmitting capability must have the transmitting capability disabled before entering the Limited Areas. If the wireless feature is to be used in the course of work, contact the Wireless Infrastructure Project for authorizations.
- **Pagers** with transmitting capabilities are not permitted in Limited Areas and some Property Protection Areas.
- Sandia-purchased BlackBerry devices are not allowed in Limited Areas.
- Call Cyber Security (4311) (844-4948) with questions concerning small electronic items.

Classified Discussions

Your Responsibility

- **Do not** discuss classified information outside Limited Areas.
- Never discuss classified or UCI over a non-secure telephone or near an in-use telephone.
- If there will be a classified discussion in a Limited Area, power off Sandia-approved cellular telephones and remove the batteries, or remove the device from the room.

For Your Information

Contact the Technical Surveillance Countermeasures Department (0301-1) for more information about cell phone policies.

Cyber Security

Cyber Security is an integral component of protecting classified information and matter at SNL/NM.

- You are responsible to protect the computer you use in the course of your work, and comply with all public laws and DOE/Sandia regulations.
- DOE and Sandia have regulations regarding information generated on computers, particularly UCI and classified information.

Key Points

- Public laws also require that you protect information generated on computers from waste, fraud, and abuse. **Other prohibitions are**:
  - Processing UCI and classified data on unauthorized computers.
  - Violating copyright and licensing restrictions.
  - Playing games and using computers for personal applications.
  - Destroying or modifying hardware, software, or data without authorization.

For Your Information

For more information on Cyber Security, or if questions arise, consult your Cyber Security Representative (CSR) in the Cyber Security Services and Technologies Department (4310).

Security Incident Management Program (SIMP)

Requirements

Reporting Security-Related Concerns

All incidents of security concerns, violations, and any other actual or suspected noncompliance that affects or potentially affects SNL security, should be reported promptly to ensure timely and appropriate reporting and follow-up.

At SNL/NM, incidents of security concern are immediately reported through the OOPS process, and then immediately to the SIMP pager, which is manned 24 hours/7 days a week, at (505) 540-2382.

In CA, call the Inquiry Official at (925) 294-3238 (SNL/CA).

Note

Caution: Do **not** discuss details of an incident via telephone, alphanumeric pager, e-mail, or voice-mail.

Preventing Further Compromise

- Preserve and protect evidence related to an incident in a manner that is appropriate for the level of classification.

Note

Evidence is considered to be classified at the same level as the classified matter to which it relates.

- For classified matter, take action to preclude further compromise or potential compromise when it is determined that information may have been lost, compromised, or is otherwise unaccounted for.
- For unclassified computer concerns (e.g., unauthorized access, viruses, junk e-mail/spam), take action to preclude further compromise or potential compromise of affected systems.

Follow Up Action

- Cooperate with Security Incident Management Program (SIMP) inquiry officials or appropriate security program management.
- **Do Not** personally investigate incidents.

Managers are responsible for ensuring that the following actions are taken for both unclassified and classified matter, as appropriate:

- Immediately upon discovery that classified matter may be lost or unaccounted for, commence an inspection for the matter.

Notes

- Inspections should be completed in a timely manner. SIMP inquiry officials or the responsible security program management personnel can assist with achieving this goal.
- Determine the root and direct causes of incidents and identify contributing factors (e.g., inadequate training, unclear security plans, lack of procedures or formal processes, inattention, or misunderstanding).
- Develop and complete corrective actions that address identified causes, the goal of which is to prevent recurrences.
- When an infraction is assessed, complete Part II of DOE F 5639.3, *Report of Security Incident/Infraction* (Word file/Acrobat file), and return the completed form to the inquiry official.
- At SNL/CA, the specified form will be completed by Security personnel.

Infractions

- Security infractions are issued in response to a breach of DOE or Sandia security rules either because of carelessness or ignorance.
  - A Sandia Security representative from SIMP conducts a fact-finding inquiry.
  - Infractions are reported to DOE.
  - A corrective action is always required after the occurrence of an infraction is issued.

Key Points

- Here are a few examples of Security Incidents that could result in an infraction being issued:
  - Leaving a classified repository unattended or unsecured.
  - Failing to account for classified matter.
  - Failing to maintain prescribed records for accountable classified matter.
  - Removing classified matter from a Security Area without proper authority.
  - Discussing classified information over unsecured telephones.
  - Not obtaining classification guidance, causing compromise of classified information.
  - Failing to properly mark classified matter as determined by classification authority.

- Improperly destroying classified information.
- Improperly transmitting classified matter (hand carries, mail, fax, phone, or e-mail).
- Improperly escorting uncleared visitors in Security Areas.
- Introducing prohibited items (such as personal computers and cellular phones) into Security Areas.
- Bringing a prohibited item into a Limited Area.

Infraction Penalty System

Security Infractions

- Employees and consultants:
  - Consequences of a Security Infraction range from coaching and counseling, to suspension or termination, in accordance with Sandia's disciplinary guidelines.
  - A supervisor is responsible for applying disciplinary action for Security Infractions.
  - A corrective action is required and shall be reported in writing to SIMP to be forwarded to DOE.
- Contractors
  - Discipline is the responsibility of the subcontractor's management.

For Your Information

If you have questions or need details concerning Security Infractions, consult the Security Incident Management Program (845-8700).

Security Depends On YOU!

Remember…

- Be aware that your access to classified matter is based on your clearance level and Need to Know.
- Protect classified matter to the best of your ability.
- Coordinate handling of classified matter with an appropriate Classified Administrative Specialist (CAS).
- Wear your badge in plain view and above the waist at all times while on Sandia property.
- Remove your badge when **not** on Sandia property (e.g., when in restaurants, grocery stores, public areas).
- **Do not** use government property for personal use.
- **Do not** bring prohibited items into security areas.
- Illegal drugs should **not** be used and are prohibited at all Sandia properties.
- Personal vehicles may **not** be brought into any SNL/NM Limited Areas unless approved.
- Interactions with foreign nationals who require access to unclassified information, programs, technologies, and SNL sites may require approval from Sandia's Foreign Interactions Office. Review the FNR Security Plan Decision Flow Diagram (http://www-irn.sandia.gov/security/dept/fio/documents/FnrSpFlow.pdf) for further information.
- Report marriage or cohabitation in writing within 45 days and name changes on the following schedule: orally, within 2 days; in writing, within the next 3 days.

Report all:

- Cases of waste, fraud, and abuse.
- Thefts of government property immediately.
- Personal foreign travel to sensitive countries.
- Foreign travel for DOE or other government agencies.
- Close and continuing contact with persons from sensitive countries.
- Arrests and all traffic fines of $250 or more in writing within 5 working days.
- Illegal or unauthorized access to sensitive matter or special nuclear material (SNM).

For Your Information

Further safeguards and security information can be found on the Sandia restricted network at http://www-irn.sandia.gov/iss/portal/.

Security Briefing Quiz

Please complete the following information
and leave this page and the quiz at the conclusion of this briefing.

Name _____ Date _____

Signature _____

Company or Organization Name _____ Last four numbers of social security _____

☐ Employee ☐ Contractor ☐ Consultant ☐ Student

Security Briefing Quiz

1. The Classified Information Nondisclosure Agreement (Standard Form 312) is an agreement between you and the federal government that:
   a. Attests to your loyalty and agreement not to disclose classified information to unauthorized sources.
   b. Agrees to provide you with a government clearance for the rest of your life
   c. Both a and b

2. As a member of the Sandia workforce your responsibilities include being aware of any special rules and/or requirements as they apply to your job.

   ☐ True ☐ False

3. Upon entering or leaving Sandia-controlled premises, all personnel are subject to search of their persons, hand-carried items, and vehicles.

   ☐ True ☐ False

4. Match the definition to the area:

_____	Property Protection Area (PPA)	a. Is established for the protection of special nuclear material.
_____	Limited Area	b. Another type of security area requiring additional Need to Know authorization, usually requiring permission be obtained before entering.
_____	Exclusion Area	c. Is established for the protection of DOE property.
_____	Material Access Area (MAA)	d. A security area having boundaries identified by barriers for the protection of classified information.

5. Non-secure telephones and fax machines, casual conversations, trash or recycled paper, and emails are all potential sources of information for adversaries to collect intelligence information.

   ☐ True ☐ False

6. Individuals with red badges (that is an uncleared Foreign National) are required to have an approved Foreign National Request Security Plan that documents which of the following:
   a. Individuals who are approved to host, co-host, and/or escort the foreign national.
   b. Approved buildings and rooms
   c. Approved access dates
   d. Approved scope of work
   e. All of the above

7. All (business or personal) travel to sensitive countries must be reported to the Foreign Travel Office.

   ☐ True ☐ False

8. Derivative Classifiers are the only persons authorized to make classification determinations.

   ☐ True ☐ False

9. Official Use Only (OUO) and Unclassified Controlled Nuclear Information (UCNI) are two of the three basic types of Unclassified Controlled Information (UCI).

   ☐ True ☐ False

10. Keeping in mind that the more sensitive the level of information, the greater the risk of damage to national security if disclosed to unauthorized sources, match the following:

_____	Top Secret	a. Unauthorized disclosure could reasonably by expected to cause undue risk to the common defense and security.
_____	Secret	b. Unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security
_____	Confidential	c. Unauthorized disclosure could reasonably be expected to cause serious damage to national security.

11. Seven steps depict the “cradle-to-grave” concept for protecting Classified Matter. Match the following steps to the associated process.

_____	Creating	a. Approved repositories (GSA approved safes and approved vaults)
_____	Accessing	b. DOE approved Mail and Shipping Channels
_____	Using	c. Marking appropriately
_____	Controlling	d. Reduced to a useless form (approved shredders)
_____	Storing	e. Marking appropriately
_____	Moving	f. Cover sheets/under personal attendance
_____	Destroying	g. Manage classified matter in classified control stations

12. An individual who has or is in the process of obtaining an "L" or "Q" clearance must report certain information. Which of the following information must be reported:
    a. verbally within 2 working days, and in writing within 3 working days, or
    b. immediately

_____ Had your wages garnished for any reason	_____ Arrested for involvement with drug or alcohol
_____ Approached or contacted by any individual seeking access to classified matter or special nuclear material.	_____ Filed for bankruptcy
_____ Changed citizenship	_____ Hospitalized for a mental illness or a mental condition, or treated for alcohol or drug abuse
_____ Contacted by persons from sensitive countries.	

13. As a host for an uncleared visitor, you are responsible for ensuring your visitor is:
    a. Badged through the Badge Office
    b. Does not have any prohibited items
    c. Remains within your visual control
    d. Does not have access to classified matter
    e. All of the above

14. When you vouch for another person, you accept responsibility and consequences of allowing that person into the area unescorted.

    ☐ True ☐ False

15. Match the following:

_____ Blue badge	a. Uncleared Foreign National, no classified access. Requires access at all times.
_____ Yellow badge	b. Q-clearance, access authorized up to SRD with Need to Know.
_____ Grey-striped badge	c. L-clearance, access authorized up to SFRD with Need to Know.
_____ Red badge	d. Uncleared U.S. citizen, no classified access. Requires escort in limited area.

16. Personal cell phones are prohibited in a limited area. Which of the following are also prohibited in a limited area:
    a. Personal iPods
    b. Personal Blackberries
    c. Personal thumb drives
    d. Personal Palm Pilots
    e. a, c, and d
    f. all of the above

17. Place the right letter in the sentence:

    Bringing in a prohibited item, leaving classified unattended, improper escorting, and sending a classified e-mail on an unclassified network, are examples of a _____ _____, and should be immediately reported to _____.

    _____ _____ are issued in response to a breach of DOE or Sandia security rules either because of carelessness or ignorance.

    a. Scandal
    b. Infraction
    c. SIMP (Security Incident Management Program)
    d. Safety
    e. Security
    f. Incident
    g. Protective Force

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN **AND THE UNITED STATES**

(Name of Individual – Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive Order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it: or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952, and 1924, Title 18, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b) (8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952, and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER *(See notice below.)*

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (*Type or Print)*

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		**THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.**	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS *(Type or Print)*		NAME AND ADDRESS *(Type or Print)*	

SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS *(TYPE OR PRINT)*	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to (1) certify that you have access to the information indicated above or (2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

***NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.**

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.